

# Week 4- Implementing Cloud Logging and Monitoring

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

College Name- Sanjivani University

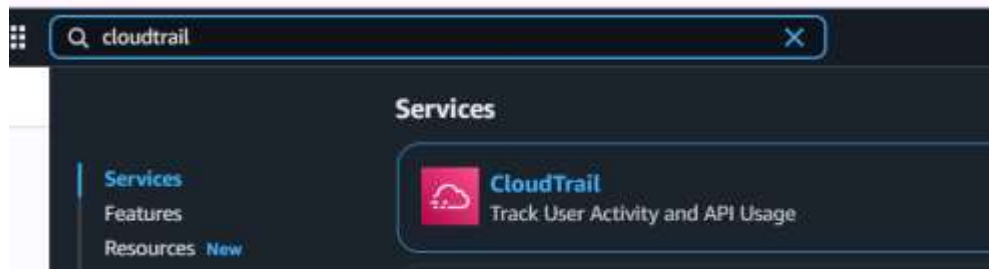
Email Id- [samruddhi.nikam\\_24ucs@sanjivani.edu.in](mailto:samruddhi.nikam_24ucs@sanjivani.edu.in)

- ❖ **Task-**
- 1) Enable CloudTrail/Cloud Audit Logs.
  - 2) Configure alerts for suspicious activity.
  - 3) Document findings.

## Step Enable Cloud Trail/ Cloud Audit Logs.

**Step 1:** Login to AWS Console

**Step 2:** Search and open CloudTrail from the Services menu.



**Step 3:** Click Create trail.



# Week 4- Implementing Cloud Logging and Monitoring

**Step 4-** Fill in trail Name cloudtrail-1, and then click create trail.

**Trail details**

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full [Create trail workflow](#).

A trail created in the console is a multi-region trail. [Learn more](#)

**Trail name**

Enter a display name for your trail.

cloudtrail-1

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

**Trail log bucket and folder**

aws-cloudtrail-logs-355433852359-b5d20482

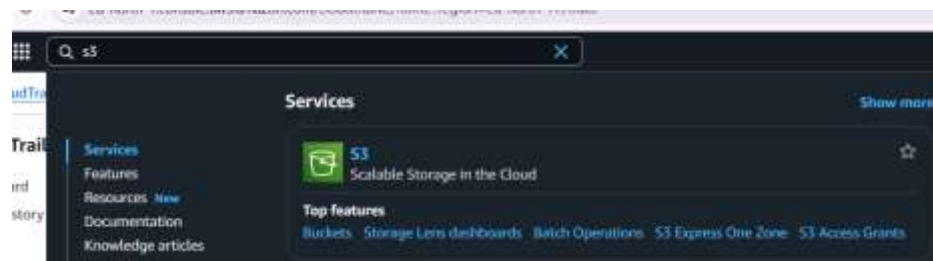
Logs will be stored in `aws-cloudtrail-logs-355433852359-b5d20482/AWSLogs/355433852359`

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

[Cancel](#) [Create trail](#)

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
<a href="#">cloudtrail-1</a>	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:355433852359:trail/cloudtrail-1	Disabled	No	<a href="#">aws-cloudtrail-logs-355433852359-b5d20482</a>	-	-	<span>Logging</span>
<a href="#">management-events</a>	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:355433852359:trail/management-events	Disabled	No	<a href="#">aws-cloudtrail-logs-355433852359-b5d20482</a>	-	-	<span>Logging</span>

**Step 5-** Set up S3 Bucket to store logs: create new bucket.

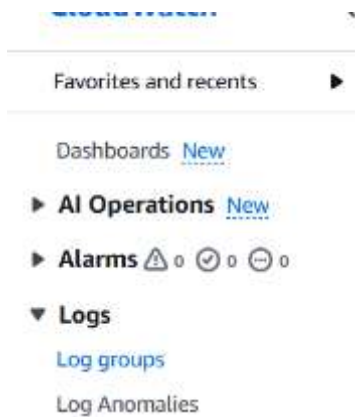


# Week 4- Implementing Cloud Logging and Monitoring

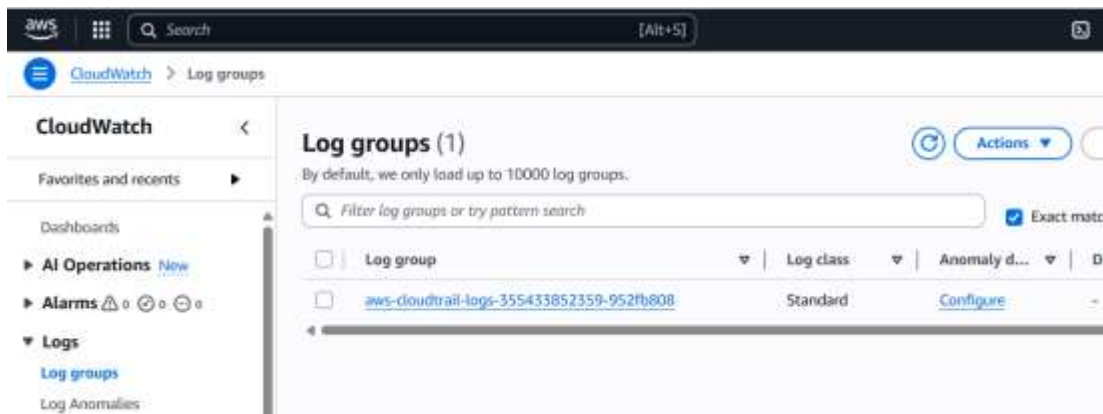
**Step 6-** Enable CloudWatch Logs, Create new Log Group: /aws/cloudtrail/logs, Allow to create IAM role automatically, then Click Create trail.

## Task 2- Configure alerts for suspicious activity.

**Step 1-**Go to CloudWatch , Log Groups

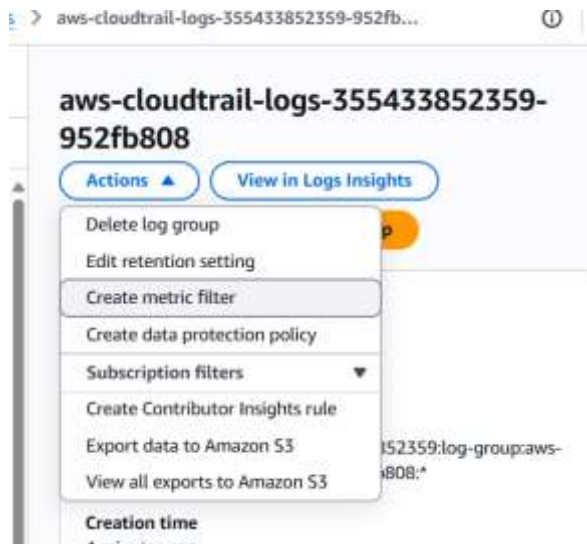


**Step 2-** Select your log group: /aws/cloudtrail/logs

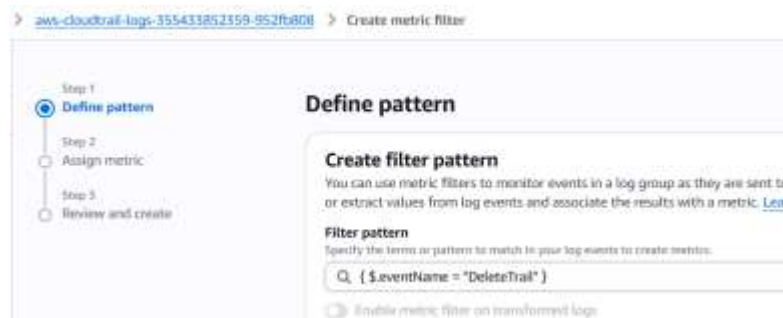


**Step 3-** Click Actions → Create Metric Filter

## Week 4- Implementing Cloud Logging and Monitoring



**Step 4-** Paste filter pattern, and then click next.



**Step 5-** next step is create filter name, enter the filter name.



**Step 6-** Then Enter the Matrix Details.

# Week 4- Implementing Cloud Logging and Monitoring

**Metric details**

**Metric namespace**  
Namespaces let you group similar metrics. [Learn more](#)

CloudTrailMonitoring Create new

Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

**Metric name**  
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)

DeleteTrailAttempts

Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(\*), dollar(\$), and space( ).

**Metric value**  
Metric value is the value published to the metric name when a Filter Pattern match occurs.

1

Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers (\$1, \$2, etc.), or named field identifiers (e.g. \$requestSize for delimited filter pattern or \$.status for JSON-based filter pattern - dollar (\$) or dollar dot (\$.) followed by alphanumeric and/or underscore (\_) characters).

**Default value - optional**  
The default value is published to the metric when the pattern does not match. If you leave this blank, no value is published when there is no match. [Learn more](#)

0

**Unit - optional**

Count

Activate Windows  
Go to Settings to activate Windows.

**Step 7-** Then click Create Matrix.

**Step 2: Metric** Edit

**Assign metric**

<b>Filter name</b> DeleteTrailFilter	<b>Metric name</b> DeleteTrailAttempts
<b>Metric namespace</b> CloudTrailMonitoring	<b>Applied on transformed logs</b> -
<b>Metric value</b> 1	<b>Default value</b> 0
<b>Unit</b> Count	

Cancel Previous Create metric filter

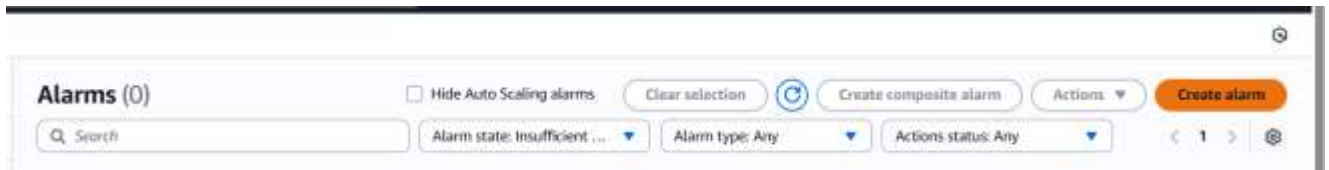
Go to Settings to activate Windows.

**Step 8-** Matrix filter Created successfully.



# Week 4- Implementing Cloud Logging and Monitoring

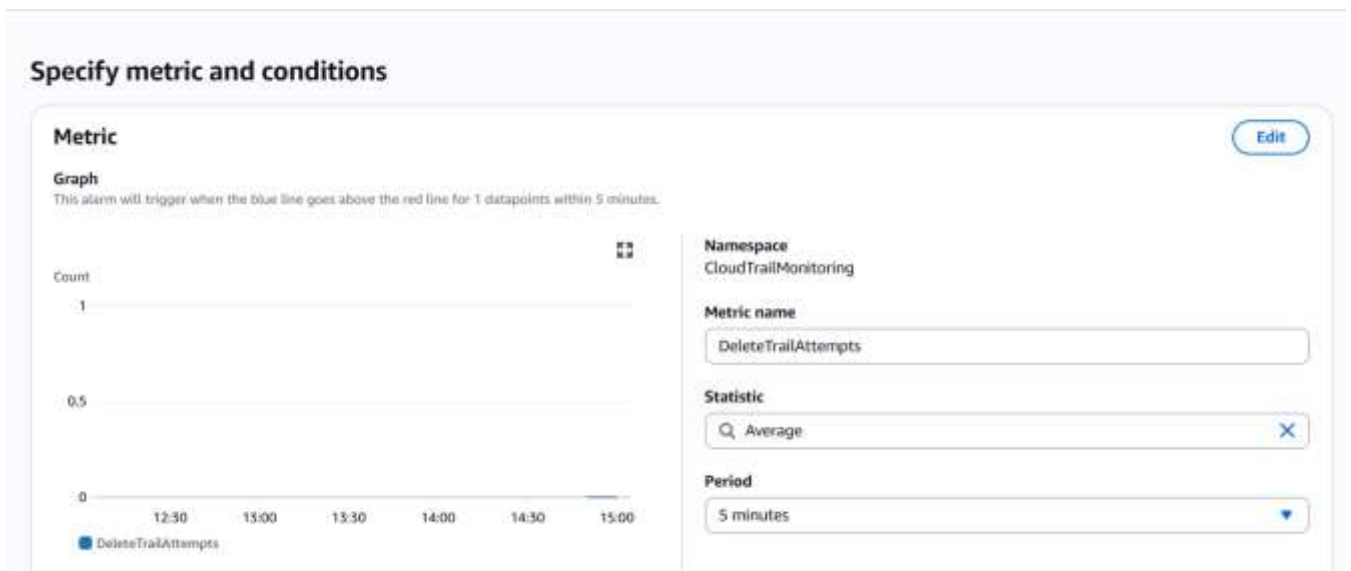
**Step 9-** Go to CloudWatch → Alarms → Create Alarm



**Step 10-** Select metric.



**Step 11-** Set threshold: Static, Condition: Greater than or equal to 1, Period: 5 minute.



# Week 4- Implementing Cloud Logging and Monitoring

**Step 12-** Set Condition, and then click Next.

The screenshot shows the 'Conditions' configuration page in the AWS CloudWatch console. Under 'Threshold type', the 'Static' option is selected. Below, the condition is set to 'Whenever DeleteTrailAttempts is...'. The comparison operator 'Greater/Equal' is selected, and the threshold value is set to '1'. The 'Additional configuration' section is collapsed. At the bottom right, there are 'Cancel' and 'Next' buttons, with an 'Activate Windows' watermark.

**Conditions**

**Threshold type**

☒ **Static**  
Use a value as a threshold

☐ **Anomaly detection**  
Use a band as a threshold

**Whenever DeleteTrailAttempts is...**  
Define the alarm condition.

☐ **Greater**  
= threshold

☒ **Greater/Equal**  
>= threshold

☐ **Lower/Equal**  
≤ threshold

☐ **Lower**  
= threshold

**than...**  
Define the threshold value.

Must be a number

► **Additional configuration**

Cancel Next

Activate Windows

**Step 13-** Add Configure Action Details.

The screenshot shows the 'Configure actions' page in the AWS CloudWatch console. Under 'Alarm state trigger', the 'In alarm' option is selected. Below, the notification is configured to be sent to an SNS topic. The 'Create new topic' option is selected, and the topic name 'Default\_CloudWatch\_Alarms\_Topic' is entered. The email endpoint 'nikamsamruddhi2006@gmail.com' is added. At the bottom right, there is a 'Remove' button and an 'Activate Windows' watermark.

alarm

**Configure actions**

**Notification**

**Alarm state trigger**  
Define the alarm state that will trigger this action.

☒ **In alarm**  
The metric or expression is outside of the defined threshold.

☐ **OK**  
The metric or expression is within the defined threshold.

☐ **Insufficient data**  
The alarm has just started or not enough data is available.

**Send a notification to the following SNS topic**  
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ **Create new topic**

☐ Use topic ARN to notify other accounts

**Create a new topic...**  
The topic name must be unique.

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (\_).

**Email endpoints that will receive the notification...**  
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

user1@example.com, user2@example.com

Remove

Activate Windows

# Week 4- Implementing Cloud Logging and Monitoring

**Step 14-** Add Alarm Details, and then click next.

**Add alarm details**

**Name and description**

Alarm name

Alarm description - optional [View formatting guidelines](#)

[Edit](#) [Preview](#)

*# This is an H1*  
*\*\*double asterisks will produce strong character\*\**  
*This is [an example](https://example.com/) inline link.*

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

[Cancel](#) [Previous](#) [Next](#)

Activate Windows

**Step 15-** Set Alarm Successfully.

Some subscriptions are pending confirmation  
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed [View SNS Subscriptions](#)

**Alarms (1)** ☐ Hide Auto Scaling alarms [Clear selection](#) [Create composite alarm](#) [Actions](#) [Create alarm](#)

Alarm state: Any Alarm type: Any Actions status: Any < 1 >

<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions	Actions
<input type="checkbox"/>	<a href="#">DeleteTrailAlarm</a>	Insufficient data	2025-07-07 15:57:08	DeleteTrailAttempts >= 1 for 1 datapoints within 5 minutes	Actions enabled <b>Warn!</b>